TECHNICAL NOTE

**Fortinet Server Authentication
Extension
Version 1.5**

FORTINET

www.fortinet.com

Trademarks
Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance
FCC Class A Part 15 CSA/CUS

Contents

Using FSAE on your network

The Fortinet Server Authentication Extension (FSAE) provides seamless authentication of Microsoft Windows Active Directory users on FortiGate units. This chapter describes how to install and configure FSAE on your Microsoft Windows network and how to configure your FortiGate unit to authenticate users using FSAE.

The following topics are included in this chapter:

- FSAE overview
- Installing FSAE on your network
- Configuring FSAE on Windows AD
- Configuring FSAE on FortiGate units
- Testing the configuration
- NTLM authentication

FSAE overview

On a Microsoft Windows network, users authenticate at logon. It would be inconvenient if users then had to enter another user name and password for network access through the FortiGate unit. FSAE provides authentication information to the FortiGate unit so that users automatically get access to permitted resources.

FortiGate units control access to resources based on user groups. Through FSAE, the Windows Active Directory (AD) groups are known to the FortiGate unit and you can include them as members of FortiGate user groups.

There are two mechanisms for passing user authentication information to the FortiGate unit:

- FSAE software installed on a domain controller monitors user logons and sends the required information directly to the FortiGate unit
- using the NTLM protocol, the FortiGate unit requests information from the Windows network to verify user authentication. This is used where it is not possible to install FSAE on the domain controller. The user must use the Internet Explorer (IE) browser.

FSAE has two components that you must install on your network:

- The domain controller (DC) agent must be installed on every domain controller to monitor user logons and send information about them to the collector agent.
- The collector agent must be installed on at least one domain controller to send the information received from the DC agents to the FortiGate unit.

Figure 1:   FSAE with DC agent
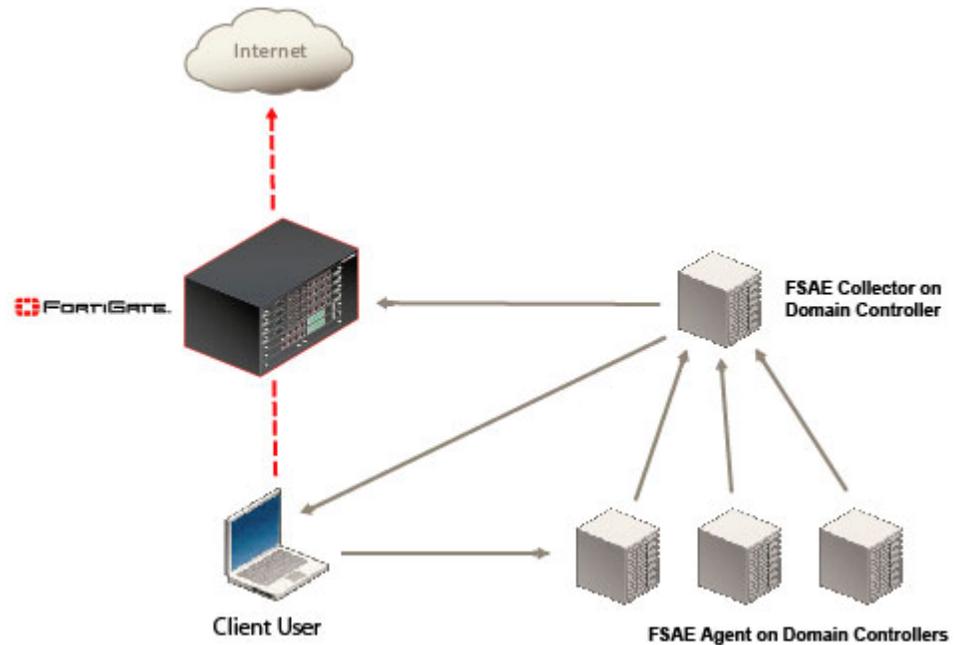
In Figure 1, the Client User logs on to the Windows domain, information is forwarded to the FSAE Collector agent by the FSAE agent on the domain controller, and if authentication is successful, the information is then sent via the collector agent to the FortiGate unit.

Figure 2:   NTLM FSAE implementation
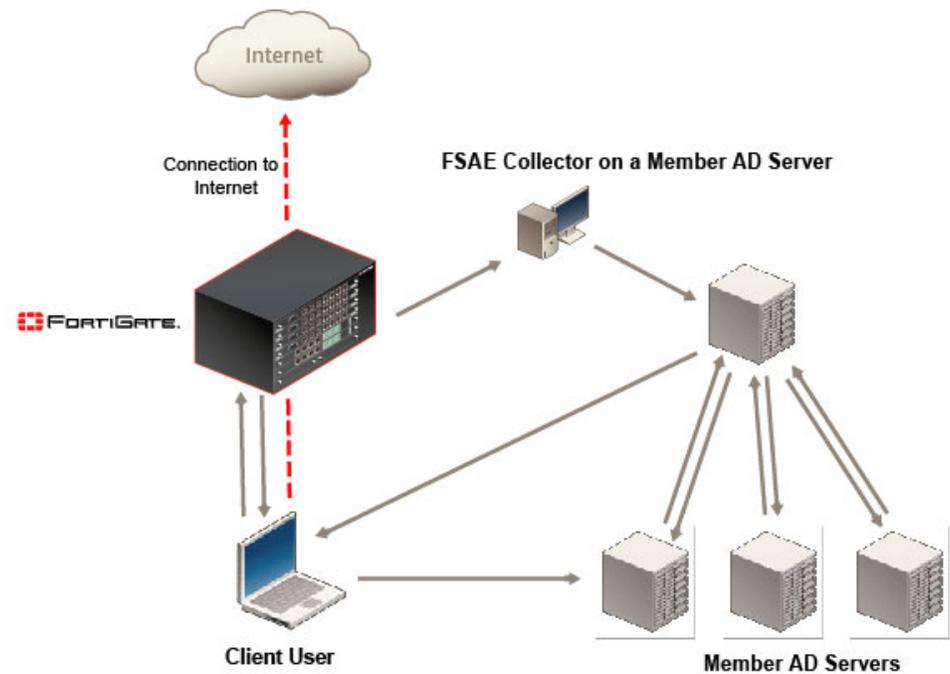
In Figure 2, the Client User logs on to the Windows domain. The FortiGate unit intercepts the request, and requests information about the user login details. The returned values are compared to the stored values on the FortiGate unit that have been received from the domain controller.

Installing FSAE on your network

FSAE has two components that you must install on your network:

- The domain controller (DC) agent, which must be installed on every domain controller
- The collector agent, which must be installed on at least one domain controller

The FSAE installer first installs the collector agent. You can then continue with installation of the DC agent, or install it later by going to **Start > Programs > Fortinet > Fortinet Server Authentication Extension > Install DC Agent**. The installer installs a DC agent on the domain controllers of all of the trusted domains in your network.

If you install the collector agent on two or more domain controllers, you can create a redundant configuration on the FortiGate unit for greater reliability. If the current collector agent fails, the FortiGate unit switches to the next one in its list of up to five collector agents.

You must install FSAE using an account that has administrator privileges. You can use the default Administrator account, but then you must re-configure FSAE each time the account password changes. Fortinet recommends that you create a dedicated account with administrator privileges and a password that does not expire.

Installing FSAE

To install FSAE, you must obtain the FortiClient Setup file from the Fortinet Support web site. Perform the following installation procedure on the computer that will run the Collector Agent. This can be any server or domain controller that is part of your network. The procedure also installs the DC Agent on all of the domain controllers in your network.

1 Create an account with administrator privileges and a password that doesn't expire. See Microsoft Advanced Server documentation for more information.

2 Log into the account that you created in Step 1.

3 Double-click the FSAESetup.exe file.

   The FSAE InstallShield Wizard starts.

4 Select Next. Optionally, you can change the location where FSAE is installed.

5 Select Next.

6 By default, FSAE authenticates users both by monitoring logons and by accepting authentication requests using the NTLM protocol.

   - If you want to support only NTLM authentication, disable the option to Monitor user logon events. Ensure that the option to Serve NTLM authentication requests is enabled.
   - If you do not want to support NTLM authentication, disable the option to Serve NTLM authentication requests. Ensure that the option to Monitor user logon events is enabled.

   You can also change these options after installation.

7 Select Next and then select Install.

8 In the Password field, enter the password for the account listed in the User Name field. This is the account you are logged into currently.

9   Select Next and then select Install.

10   When the FSAE InstallShield Wizard completes, ensure that Launch DC Agent Install Wizard is enabled and select Finish.

The FSAE - Install DC Agent wizard starts.

11   Check the Collector Agent IP address.

If the Collector Agent computer has multiple network interfaces, ensure that the one that is listed is on your network. The listed Collector Agent listening port is the default. You should change this only if the port is already used by some other service.

12   Select Next.

13   Check the list of trusted domains and select Next.

If any of your required domains are not listed, cancel the wizard and set up the proper trusted relationship with the domain controller. Then run the wizard again by going to **Start > Programs > Fortinet > Fortinet Server Authentication Extension > Install DC Agent**.

14   Optionally, select users that you do not want the DC Agent to monitor logon status for. These users will not be able to authenticate to FortiGate units using FSAE. You can also do this later. See "Configuring FSAE on Windows AD" on page 8.

15   Select Next.

16   Optionally, clear the check boxes of domain controllers on which you do not want to install the FSAE DC Agent.

17   Select Next.

18   Select Yes when the wizard requests that you reboot the computer.

Note: If you reinstall the FSAE software on this computer, your FSAE configuration is replaced with default settings.

If you want to create a redundant configuration, repeat this procedure on at least one other domain controller.

Note: When you start to install a second collector agent, when the Install Wizard dialog appears the second time, cancel it. From the configuration GUI, the monitored domain controller list should show your domain controllers unselected. Select the ones you wish to monitor with this collector agent, and click Apply.

Before you can use FSAE, you need to configure it on both Windows AD and on the FortiGate units. See the next section, "Configuring FSAE on Windows AD", and "Configuring FSAE on FortiGate units" on page 14.

Configuring FSAE on Windows AD

On the FortiGate unit, firewall policies control access to network resources based on user groups. Each FortiGate user group is associated with one or more Windows AD user groups.

FSAE sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units. To avoid this problem, you can configure the FSAE collector agent to send logon information only for groups named in the FortiGate unit's firewall policies.

On each domain controller that runs a collector agent, you need to configure

- Windows AD user groups
- collector agent settings, including the domain controllers to be monitored
- the collector agent Global Ignore list
- the collector agent FortiGate Group Filter for each FortiGate unit

The following client/server operating systems can be used:

Server: Microsoft Windows 2000, Microsoft Windows 2003 (32-bit and 64-bit)

Client: Microsoft Windows 2000 Professional, Microsoft Windows XP Professional

Configuring Windows AD server user groups

FortiGate units control access at the group level. All members of a group have the same network access as defined in FortiGate firewall policies. You can use existing Windows AD user groups for authentication to FortiGate units if you intend that all members within each group have the same network access privileges. Otherwise, you need to create new user groups for this purpose.

If you change a user's group membership, the change does not take effect until the user logs off and then logs on again.

FSAE sends only Domain Local Security Group and Global Security Group information to FortiGate units. You cannot use Distribution group types for FortiGate access. No information is sent for empty groups.

Refer to Microsoft documentation for information about creating groups.

## Configuring collector agent settings

You need to configure

- the Windows AD domain controllers to monitor
- the Windows AD users to ignore because they do not participate in firewall authentication on any FortiGate unit
- the Windows AD group information to send to each FortiGate unit

You can also alter default settings and settings you made during installation.

To configure the FSAE collector agent

1   From the Start menu select **Programs > Fortinet >
Fortinet Server Authentication Extension > Configure FSAE**.
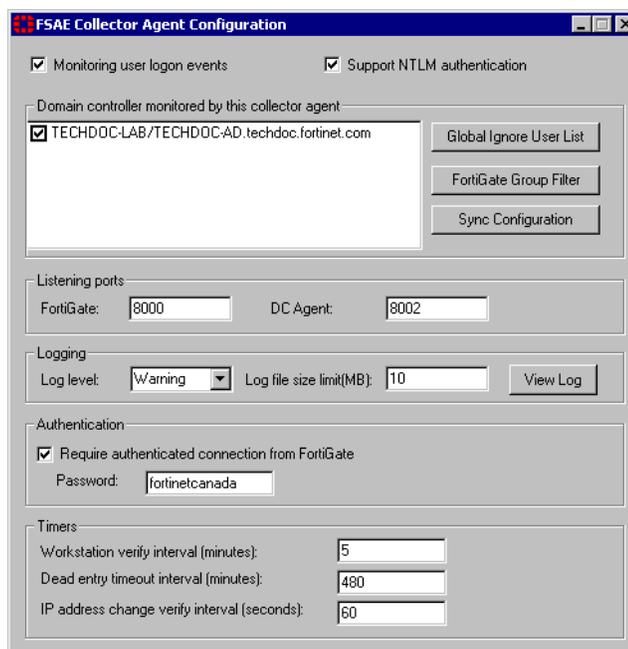
2   Enter the following information and then select Save and Close.

Monitoring user logon events	Enable to automatically authenticate users as they log on to the Windows domain.
Support NTLM authentication	Enable to facilitate logon of users who are connected to a domain that does not have the DC Agent installed.
Domain controller monitored	Select the domain controllers that you want to monitor for users logging on.
Global User Ignore List	Exclude users such as system accounts that do not authenticate to any FortiGate unit. See "Configuring the Global Ignore List" on page 11.
FortiGate Group Filter	Configure group filtering for each FortiGate unit. See "Configuring FortiGate group filters" on page 11.
Sync Configuration	Copy this collector agent's Global Ignore List and Group Filters to the other collector agents to synchronize the configuration. You are asked to confirm synchronization for each collector agent.
Listening ports	You can change port numbers if necessary.
FortiGate	TCP port for FortiGate units. Default 8000.
DC Agent	UDP port that DC Agents use. Default 8002.
Logging	
Log level	Select the minimum severity level of logged messages.
Log file size limit	Enter the maximum size for the log file in MB.
Authentication	
Require authenticated connection from FortiGate	Select to require the FortiGate unit to authenticate before connecting to the Collector Agent.

Password	Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is "fortinetcanada".
Timers	
Workstation verify interval	Enter the interval in minutes at which FSAE checks whether the user is still logged in. The default is every 5 minutes.
	If ports 139 or 445 cannot be opened on your network, set the interval to 0 to disable the check. See "Configuring TCP ports" on page 13.
Dead entry timeout interval	Enter the interval in minutes after which FSAE purges information for user logons that it cannot verify. The default is 480 minutes (8 hours).
	Dead entries usually occur because the computer is unreachable (in standby mode or disconnected, for example) but the user has not logged off.
	You can also disable dead entry checking by setting the interval to 0.
IP address change verify interval	FSAE periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change. This does not apply to users authenticated through NTLM. Enter the verification interval in seconds. IP address verification prevents users from being locked out if they change IP addresses. You can enter 0 to disable the IP address check if you use static IP addresses.
Save & Close	Save the modified settings and exit.
Apply	Apply changes now.
Default	Change all settings to the default values.
Help	View the online Help.

Note: To view the version and build number information for your FSAE configuration, click the Fortinet icon in the upper left corner of the Fortinet Collector Agent Configuration screen and select "About FSAE configuration".

Configuring the Global Ignore List

The Global Ignore List excludes users such as system accounts that do not authenticate to any FortiGate unit. The logons of these users are not reported to FortiGate units.

To configure the Global Ignore List

1   From the Start menu select **Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE**.

2   Select Global Ignore List.

3   Expand each domain and select the users to ignore.

4   Select Save.

Configuring FortiGate group filters

FortiGate filters control the user logon information sent to each FortiGate unit. You need to configure the list so that each FortiGate unit receives user logon information for the user groups that are named in its firewall policies.

The filter list is initially empty. You need to configure filters for your FortiGate units using the Add function. At minimum, you can create a default filter that applies to all FortiGate units that do not have a specific filter defined for them.

Note: If no filter is defined for a FortiGate unit and there is no default filter, the collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing the amount of memory the unit uses to store the group list.

To view the FortiGate Filter List

1   From the Start menu select **Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE**.

2   Select FortiGate Group Filter.

The FortiGate Filter List opens.
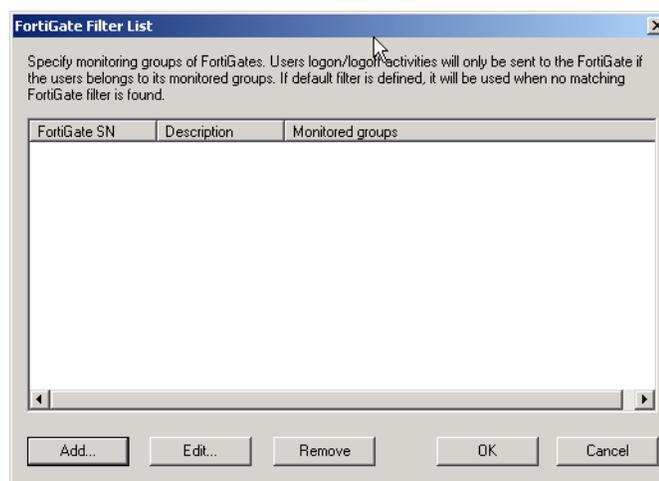
FortiGate SN	The serial number of the FortiGate unit to which this filter applies.
Description	An optional description of the role of this FortiGate unit.
Monitored Groups	The Windows AD user groups that are relevant to the firewall policies on this FortiGate unit.
Add	Create a new filter. See "To configure a FortiGate group filter" on page 12.
Edit	Modify the filter selected in the list.
Remove	Remove the filter selected in the list.
OK	Save the filter list and exit.
Cancel	Cancel changes and exit.

To configure a FortiGate group filter

1   From the Start menu select **Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE**.
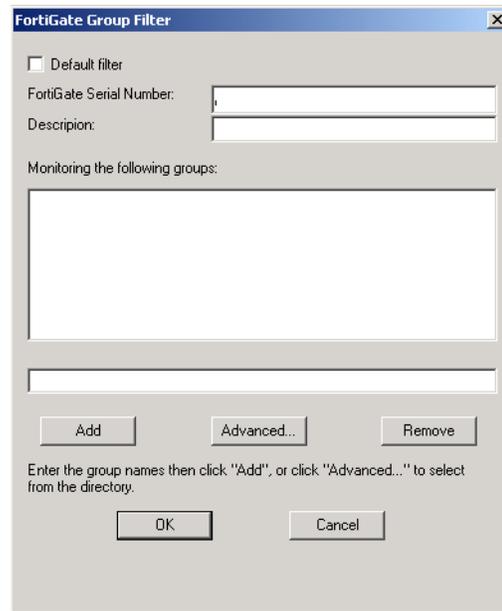
2   Select FortiGate Group Filter.

3   Select Add to create a new filter. If you want to modify an existing filter, select it in the list and then select Edit.

4   Enter the following information and then select OK.

Default	Select to create the default filter. The default filter applies to any FortiGate unit that does not have a specific filter defined in the list.
FortiGate Serial Number	Enter the serial number of the FortiGate unit to which this filter applies. This field is not available if Default is selected.
Description	Enter a description of this FortiGate unit's role in your network. For example, you could list the resources accessed through this unit. This field is not available if Default is selected.
Monitor the following groups	The collector agent sends the FortiGate unit user logon information for the Windows AD user groups in this list. You edit this list using the Add, Advanced and Remove buttons.
Add	In the preceding single-line field, enter the Windows AD domain name and user group name in the format "Domain/Group" and then select Add. If you don't know the exact name, use the Advanced button instead.
Advanced	Select Advanced, select the user groups from the list, and then select Add.
Remove	Remove the user groups selected in the monitor list.

Configuring TCP ports

Windows AD records when users log on but not when they log off. For best performance, FSAE monitors when users log off. To do this, FSAE needs read-only access to each client computer's registry over TCP port 139 or 445. At least one of these ports should be open and not blocked by firewall policies.

If it is not feasible or acceptable to open TCP port 139 or 445, you can turn off FSAE logoff detection. To do this, set the collector agent Workstation verify interval to 0. FSAE assumes that the logged on computer remains logged on for the duration of the collector agent Dead entry timeout interval. By default this is eight hours. For more information about both interval settings, see "Timers" on page 11 in the "Configuring collector agent settings" section.

Configuring FSAE on FortiGate units

To configure your FortiGate unit to operate with FSAE, you

• specify the Windows AD servers that contains the FSAE collector agents

• add Active Directory user groups to new or existing FortiGate user groups

• create firewall policies for Windows AD Server groups

• optionally, specify a guest protection profile to allow guest access

Specifying your collector agents

You need to configure the FortiGate unit to access at least one FSAE collector agent. You can specify up to five Windows AD servers on which you have installed a collector agent. The FortiGate unit accesses these servers in the order that they appear in the list. If a server becomes unavailable, the unit accesses the next one in the list.

To specify collector agents

1 Go to **User > Windows AD** and select Create New.

2 Enter the following information and select OK:

|	
Name	Enter a name for the Windows AD server. This name appears in the list of Windows AD servers when you create user groups.
FSAE Collector IP	Enter the following information for up to five collector agents.
IP Address	Enter the IP address of the Windows AD server where this collector agent is installed.
Port	Enter the TCP port used for Windows AD. This must be the same as the FortiGate listening port specified in the FSAE collector agent configuration. See "Configuring FSAE on Windows AD" on page 8.
Password	Enter the password for the collector agent. This is required only if you configured your FSAE collector agent to require authenticated access. See "Configuring FSAE on Windows AD" on page 8.

Viewing information imported from the Windows AD server

You can view the domain and group information that the FortiGate unit receives from the AD Server. Go to **User > Windows AD**.

Figure 3:   List of groups from Active Directory server
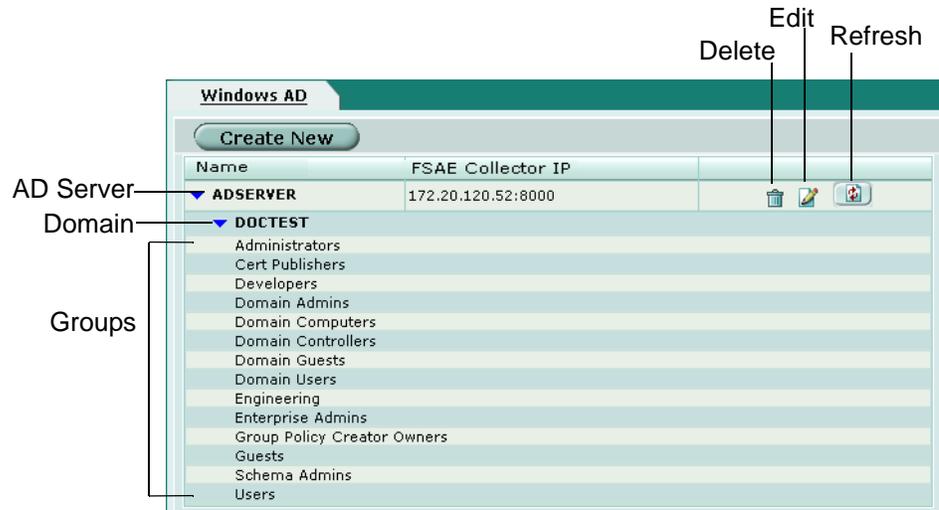
Create New	Add a new Windows AD server.
Name	
AD Server	The name defined for the Windows AD server.
Domain	Domain name imported from the Windows AD server.
Groups	The group names imported from the Windows AD server.
FSAE Collector IP	The IP address of the Windows AD server
Delete icon	Delete this Windows AD server definition.
Edit icon	Edit this Windows AD server definition.
Refresh icon	Get user group information from the Windows AD server.

Creating user groups

You cannot use Active Directory groups directly in FortiGate firewall policies. You must add Active Directory groups to FortiGate user groups.

An Active Directory group should be belong to only one FortiGate user group. If you assign it to multiple FortiGate user groups, the FortiGate unit recognizes only the last user group assignment.

To create a user group for FSAE authentication

1   Go to **User > User Group**.

2   Select Create New.

The New User Group dialog box opens.

Figure 4:   New User Group dialog box

3   In the Name box, enter a name for the group, Developers, for example.

4   From the Type list, select Active Directory.

5   From the Protection Profile list, select the required protection profile.

6   From the Available Users list, select the required Active Directory groups.

Using the CTRL or SHIFT keys, you can select multiple groups.

7   Select the green right arrow button to move the selected groups to the Members list.

8   Select OK.

Creating firewall policies

Policies that require FSAE authentication are very similar to other firewall policies. Currently, only one single authentication firewall policy can be configured if the source interface/source IP pair is the same.

To create a firewall policy for FSAE authentication

1   Go to **Firewall > Policy** and select Create New.

2   Enter the following information:

Source interface and address	as required
Destination interface and address	as required
Schedule	as required
Service	ANY
Action	ACCEPT
NAT	as needed

3   Select Authentication and then select Active Directory from the adjacent list.

4   Select the required user group from the Available Groups list and then select the right arrow button to move the selected group to the Allowed list.

You can select multiple groups using the CTRL or SHIFT keys.

5   Select OK.

Allowing guests to access FSAE policies

Optionally, you can allow guest users to access FSAE firewall policies. Guests are users unknown to the Windows AD network and servers that do not log on to a Windows AD domain. To allow guest access, use the FortiGate GUI or CLI to specify a guest protection profile for your FSAE firewall policy. For example

```
config firewall policy
   edit FSAE_policy
      set fsae-guest-profile strict
   end
```

You can specify any existing protection profile. If you prefer, you can create a custom protection profile to assign to guest users. For more information, see the Firewall Protection Profile chapter of the *FortiGate Administration Guide*.

Testing the configuration

To verify that you have correctly configured FSAE on your network and on your FortiGate units:

1 From a workstation on your network, log on to your domain using an account that belongs to a group that is configured for authentication on the FortiGate unit.

2 Try to connect to the resource that is protected by the firewall policy requiring authentication via FSAE.

You should be able to connect to the resource without being asked for username or password.

3 Log off and then log on using an account that does not belong to a group you have configured for authentication on the FortiGate unit.

4 Try to connect to the resource that is protected by the firewall policy requiring authentication via FSAE.

Your attempt to connect to the resource should fail.

NTLM authentication

In system configurations where it is not possible to install FSAE clients on all AD servers, the FortiGate unit must be able to query the AD servers to find out if a user has been properly authenticated. This is achieved using the NTLM messaging features of Active Directory and Internet Explorer.

Understanding the NTLM authentication process

1 The client (user) attempts to connect to an external HTTP resource (internet) and issues an unauthenticated request via the FortiGate unit.

2 The FortiGate is aware that this client has not authenticated previously, so responds with a `401 Unauthenticated` status code, and tells the client which authentication method to come back with via the header: `Proxy-Authenticated: NTLM`. The session is dismantled.

3   The client connects again, and issues a GET-request, with a
`Proxy-Authorization: NTLM <negotiate string>` header.
`<negotiate-string>` is a base64-encoded NTLM Type 1 negotiation packet.

4   The FortiGate unit replies with a `401 "proxy auth required"` status code,
and a `Proxy-Authenticate: NTLM <challenge string>` (a bae64-
encoded NTLM Type 2 challenge packet. In this packet is the challenge nonce, a
random number chosen for this negotiation that is used once and prevents replay
attacks.

Note: It is vital that the TCP connection is kept alive, as all subsequent authentication-
related information is tied to the TCP connection. If it is dropped, the authentication process
must start again from the beginning.

5   The client sends a new GET-request with a header:`Proxy-Authenticate:
NTLM <authenticate string>`, where `<authenticate string>` is a
NTLM Type 3 Authentication packet that contains:

- user name and domain
- the challenge nonce encoded with the client password (it may contain the
challenge nonce twice using different algorithms)

6   The FortiGate unit checks with the FSAE client (over port 8000) to see if the
authentication hash matches the one on the domain controller. The FortiGate unit
will deny the authentication via a 401 return code and prompt for a username and
password, or return an "OK" response and the Window's group name(s) for the
client.

Unless the TCP connection is broken, no further credentials are sent from the
client to the proxy.

7   The FortiGate unit uses the group name(s) to match a protection profile for the
client, and establishes a temporary firewall policy that allows future traffic to pass
through the FortiGate unit.

Note: If the authentication policy reaches the authentication timeout period, a new NTLM
handshake occurs.

www.fortinet.com

FÜRTINET.

www.fortinet.com